黑客之死

2017-09-21张坤（ID：破天）行长叠报

开篇之前，先介绍一下自己的职场经历和安全行业经历，并无意抨击或贬低任何一种安全从业人员。仅对最近两年安全圈或者黑客圈、白帽子圈发表一下自己的看法。

初涉安全圈

08年因为《魔域》账号的丢失，想着怎么找回，后来发现找回无望，又想着弄明白别人是怎么做的，后来又想弄明白怎么才能不被盗号，就这样一条线拉着一条线，慢慢把我拉上了现在的职业道路。

就这样初涉安全圈，干脆叫黑客圈（不想再解释黑客 白帽子啥的，**黑客并无贬义**），上面说安全圈，干脆叫黑客圈，为什么这样说？理由很简单：当时安全人员没地方吃饭，没有就业岗位，只能求其次选择了除了安全更擅长的岗位。
当时安全人员求职，第一职位是安全，第二职位是运维，第三职位是数据库。

安全经历

在这个大环境下，我经历了金融服务商（两年）、老牌国企金融机构（六年）、互联网金融机构和大型互联网机构。

在金融服务商，把安全概念带进了机房和客户服务，在金融机构，有幸负责了企业的安全、网络管理和系统规划建设工作。

六年通过证券业协会的平台、各种业内交流、各种出差学习和实践机会，迅速成长为从一个只会挖洞、提一些不切实际的安全小白成长为可以独当一面的安全人，直至今日经历了从传统金融公司到互联网金融公司再到互联网公司的跨步。

“安全圈现在就是娱乐圈”，最近两三年最直观的感受，哗众取宠，争强好胜，甚至以斗图、互怼、肉鸡量、shell量等等来炫耀，我不知道这样对不对，可这不是我印象里的安全圈，更不是想要的安全圈。

三个黑客时代

我经历过三个黑客时代，并有幸得“explorer”启蒙，并有幸和**“龙腾风云”、“亮哥”、“alpha”**共事交流，也很荣幸得到其他未提名的领导朋友的指点和帮助，算是我安全圈的贵人。

第一个黑客时代的人，是很值得我们学习得人，不只是技术，他们现在要么创业成功，要么成为某大型公司的安全负责人，要么是某安全公司的负责人。他们低调，有技术，有格局，见证过绿盟站、黑基、乌云等。

第一代黑客

- 综合素质强，安全设备、安全研发、数据库、系统、应用、中间件、业务系统、语言、网络架构、系统规划建设等颇有涉猎
- 懂得针对业务特点、企业实际环境设计符合现状的安全体系架构和安全技术架构
- 有格局，有技术，有管理能力和个人资源
- 对各大厂商的产品、技术甚至商务都如数家珍

第二代黑客

- 绝大数从事安全相关工作，一部分身兼数岗，网络和安全、运维和安全
- 熟悉常见系统架构和风险
- 多年从业有自己的认识，但缺少对系统性的理解
- 可以负责安全团队的部分内容

第三代黑客

- 挖洞
- 挖洞
- 挖洞
- 缺少专业知识和系统化概念
- 擅长斗图、getshell、各种互联网找洞

- 职业规划不明确，自身定位价值偏差

个人的浅见，三代黑客代表了中国三代黑客文化，更代表了必不可少的黑客成长历程，从挖洞入门，通过沙龙交流学习，缺少的专业知识通过各种充电来提升，成长为安全团队的一员，在团队内互相帮扶成长，各种项目、经验和能力的提升，再加上个人职位方向和好的契机，又恰巧有一伯乐，走上自己期望的岗位。这是我认为的黑客成长道路，我的很多朋友包括我自己，沿着各条路摸索着成长。

在乌云笼罩的日子，一个帖子如果不能有绝对的干货，一定会被pass；一个漏洞提交，如果详细度不足以让审帖人员顺利复现，一定会被pass；厂商多久不修复，一定会被曝光。

黑客乌托邦

大家不为钱，不为名气，纯为技术，有几十个rank值是极大的荣幸，算是黑客乌托邦吧。不以成败论英雄，不以对错论好坏。安全平台通过短短的时间吸引了极多的所谓白帽子，通过各种宣传、运营和各种活动带给了白帽子们极大的荣誉感和归属感，这当然是极好的，通过可控的技术平台和统一出口来监管可能会踩红线的行为，并有资金奖励，让白帽子们满足于挖洞，且专（只）于挖洞，在带给大家机会和舞台的时候，也带来了一些错误认识，比如自身价值定位等，无数次听src人员抱怨现在白帽子太难伺候，提交漏洞扔出来就得给过，让他写详细点就想吃人的样子。

新起点

中国的网络安全法，成立于2017年六月一日，说明我们的安全开始被国家重视，虽然现在被很多人说“贵圈很乱”，我想只是因为我们还小，**我们需要成长，更需要良好的环境成长，需要在良好的教育环境成长**，最终会干美国干俄罗斯干韩国干印度，成为真正的黑客！

在我国市场上，安全被国家重视立法今年才开始，相比较其他发达国家，起步较晚，立法、专业建设等都比较晚，所以专业人才保有量较少，人才需求量猛增带来了种种问题，对企业来讲岗位需求不明确、安全人员价值开发不完全、资源配备不均衡、安全机构成为摆设，个人来讲应职人员滥竽充数、社会人员浮躁无法正视自己的问题，技术学习以漏洞利用、肉鸡、shell或者干脆攻击为主。

几点建议

我资历尚浅，说这些心有惶恐，每天看着圈内各种怪相还是想衷心给大家几个建议：

1、安全不只是挖洞，甚至挖洞在乙方的工作量都占不到一般，更遑论甲方
2、不要那么浮躁，静下心学些真正的安全技术
3、多写点东西总没错，安全本就是综合性的能力
4、进入安全圈，不是认识几个人，参加几次沙龙、提交几个漏洞、写过几篇挖洞或者工具利用的文章

现在大家停留在最基础的逻辑洞、通用洞或NDAY漏洞上，去互联网扫，比如strust2 045 052等，用工具一扫一堆，这些漏洞真的有价值吗？有，但还不够，如果上升到架构设计规范、上升到安全标准体系、上升到通用安全基线是不是可以做的更好？

针对社会白帽子和企业安全员，也针对挖洞和企业安全阐述一点自己的看法：

1、挖洞，现在大家停留在最基础的逻辑洞、通用洞或NDAY漏洞上，去互联网扫，比如strust2 045 052等，用工具一扫一堆，这些漏洞真的有价值吗？有，但还不够，如果上升到架构设计规范、上升到安全标准体系、上升到通用安全基线是不是可以做的更好？

2、关于企业安全，企业安全按企业类型划分分为，传统企业安全、互联网企业安全，企业安全涵盖了五大领域基本包括网络安全、业务安全、安全体系建设、风控合规及审计、业务持续性管理，这五大领域相互独立又错综交叉，互相促进又互相克制，细分工作内容如下：

- 信息安全管理：制度、流程 整体策略等

- 基础架构与网络安全：制度、流程 整体策略等

- 基础架构与网络安全：IDC生产网络的各种链路、设备服务器、服务端程序、中间件、DB，漏扫 补丁修复 ACL 安全配置 N/H ips等

- 应用与交付安全：对各BG、业务的产品进行应用级风险评估代码审计透测试 代码框架的安全功能和应用级防火墙、IPS等，包括SDL等

- 业务安全：账号安全 交易风控 征信 反价格爬虫 反作弊饭bot程序 反欺诈 反钓鱼 反垃圾信息 舆情监控 防外挂 打击黑产 安全情报 态势感知等

- 企业认证和合规标准：等级保护测评认证、国内的ISO2700x、国外的BS7799和BS25999等

- 企业级安全管理：战略级安全规划建设、安全预算、TCO/ROI等

作为黑客的你，看完上面的内容还觉得挖洞只能做到这样了吗？除了挖洞我们真的没得做了吗？

15060541.26573

微信扫一扫

关注该公众号